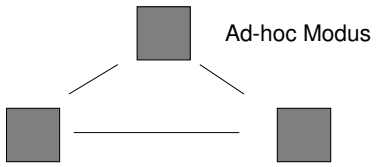
WLAN

Wie unsicher isses eigentlich ?

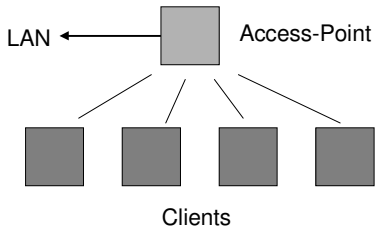
WLAN

- Steigende Verbreitung
- Alle Centrino Notebooks sind WLAN fähig
- Unterschiedliche Hard - und Software mit höchstunterschiedlichen Leistungsmerkmalen
- Hot Spots an Flughäfen, Bahnhöfen usw.

Peer - to - Peer Kommunikation



Infrastruktur-Modus



Netzwerkname (SSID)

- Standardmässig kann ein Netzwerkname vergeben werden (ESSID [Extended] Service Set Identity).
- 2 Betriebsarten
  - Wird durch den Nutzer „Any“ vergeben, akzeptiert das Bauteil beliebige SSIDs.
  - Sonst wird der eingetragene Netzwerkname überprüft und es werden nur Komponenten mit der gleichen SSID zugelassen.

Netzwerkname (SSID)

- Bei Übergabe zwischen 2 Access Points wird mit der SSID der nächste Point gefunden
- Die SSID wird im Klartext über das Netz gesendet
- Einige (!) Access Points haben die Option die SSID im Broadcast zu verhindern (Nicht Standard)

MAC Adresse

- Prinzipiell ist es möglich, eine Liste von MAC Adressen zu definieren, die mit dem Access Point kommunizieren dürfen
- Die Liste(n) müssen händisch gepflegt werden
- Darüber hinaus können MAC Adressen natürlich geändert werden

WEP

- Wired Equivalent Privacy
- Soll Vertraulichkeit und Integrität der übertragenen Daten sichern und die Authentisierung des Endgerätes - nicht des Nutzers - durchführen

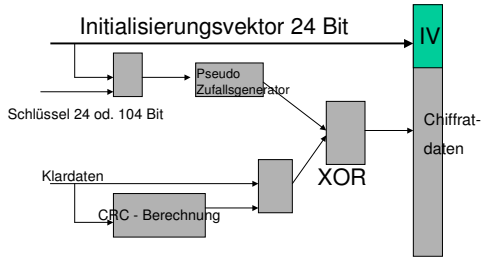
WEP

- Basiert auf einem Stromchiffre RC4 mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor in Chiffratdaten umgewandelt werden
- Der Schlüssel ist eine Zeichenkette der wahlweise 40 oder optional 104 Bit gross ist und den Clients und den Access Points vorab zur Verfügung gestellt werden muss

WEP

- Für das gesamte LAN wird ein Schlüssel verwendet
- Der IV wird vom Absender gewählt und wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und übertragen

Blockdarstellung



Authentisierung

- WEP kennt 2 Modi zur Authentisierung
- Open - keine Authentisierung
- Shared Key - Der Access Point sendet 128 zufällige Bytes an den Client, der verschlüsselt die Bytes und sendet sie zurück. Wenn der AP in der Lage ist, die Nachricht zu entschlüsseln, hat sich der Client erfolgreich authentisiert.

SSID Broadcast

- Einige der AP bieten die Möglichkeit, das Senden der SSID zu unterbinden um das WLAN gegenüber Unbefugten zu verstecken (Closed System).
- Wirkt gegen einige der frei verfügbaren Tools, die SSID kann jedoch mit einigen Tools aus den Steuersignalen ermittelt werden.

24.10.2004

Key - Management

- Der Schlüssel muss in allen WLAN Komponenten (Clients & AP) identisch sein
- Führt nicht unbedingt dazu, dass er allzu oft geändert wird ;-)
- Der Verlust eines Schlüssel führt sofort dazu, das dass komplette Netz kompromittiert wird

24.10.2004

Schlüssellänge

- Die Länge von 40 Bit ist nicht ausreichend. Bei einem aufgezeichneten Chiffrat kann der Key durch probe-entschlüsseln mit einem normalen PC schnell entschlüsselt werden
- Lediglich 104 Bit gelten als ausreichend

24.10.2004

Länge des IV

- Da der Key für einige Zeit als konstant angenommen werden kann, ist es möglich den IV mit einer Länge von 24Bit in relativ kurzer Zeit zu knacken.
- Es sind maximal 16,8 Mio verschiedene Ivs generierbar

24.10.2004

Alternative zu WEP

- WPA (Wi-Fi Protected Access) ist eine Zwischenlösung bis zur Veröffentlichung des Standards IEEE 802.11i.
- Verwendet AES statt der Stromchiffre

24.10.2004

AP

- Der AP muss sich nicht authentisieren
- Es ist durchaus möglich, einen AP aufzustellen um einfach mal zu testen, „was der Client so zu bieten hat“
- Voraussetzung ist natürlich der Key

24.10.2004

Standard

- IEEE 802.11b und 802.11g sind derzeit die gültigen Standards in diesen sind die vorher beschriebenen Features definiert
- Man sollte es vermeiden die beiden Standards zu mischen, denn ein AP kann nur mit einem Standard arbeiten.

24.10.2004

Zitat

„Bei der drahtlosen Vernetzung – der Übertragung von Daten an einen beliebigen Empfänger im Funkbereich – sind weit reichende Auswirkungen in Bezug auf die Sicherheit zu bedenken. Intel führte aus diesem Grund ein VPN-Gateway (virtuelles privates Netzwerk) ein, das sich zur Bereitstellung der bei Intel benötigten kompromisslosen Sicherheit des WEP-Protokolls nach 802.11b bedient. Mittels der VPN-Ebene werden starke Authentifizierungs- und Verschlüsselungsmechanismen zwischen den drahtlosen Zugriffspunkten und dem Netzwerk errichtet. VPN kann auch im vorhandenen Kabelnetzwerk implementiert werden, so dass zum Schutz des Arbeitsplatzes dieselbe Technologie zum Einsatz kommt. Dank VPN besteht für Benutzer die Möglichkeit der nahtlosen Interaktion mit einem beliebigen Netzwerk, und Intel verfügt über die Datensicherheit, die das Unternehmen benötigt.“
Quelle:http://www.intel.com/business/enterprise/emea/deu/bss/infrastructure/security/vpn_wep.htm

24.10.2004